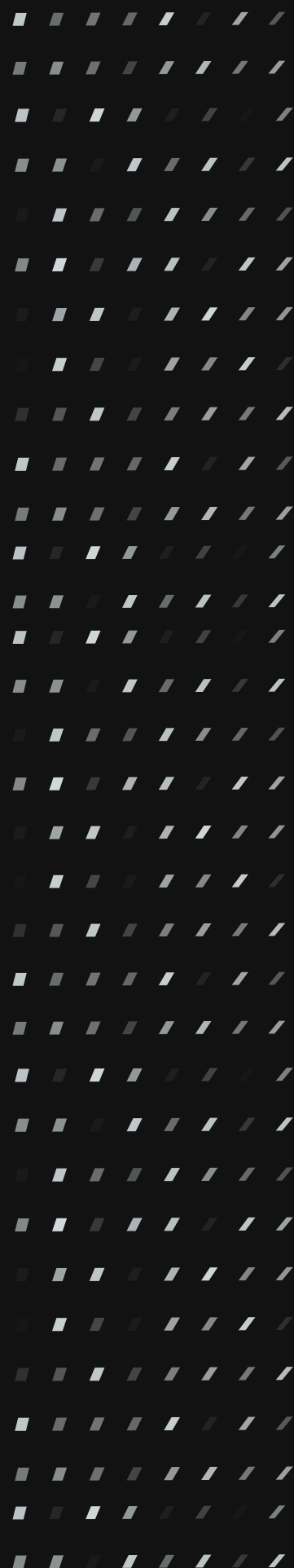


LIVRE BLANC

Hiérarchiser les projets d'automatisation du réseau en fonction des besoins



Comme de nombreux ingénieurs réseau, on vous demande certainement d'en faire plus, plus rapidement qu'auparavant, et sans interférer avec les autres activités de l'entreprise. Dans bien des entreprises, l'infrastructure réseau continue de s'étendre pour répondre à la croissance des communications, des applications et des capacités de stockage des données. Dans le même temps, la plupart des équipes d'ingénierie réseau n'obtiennent pas les effectifs supplémentaires dont elles ont besoin pour tenir le rythme ou même remplacer les collaborateurs talentueux qui partent.

Si l'on réunit tous ces éléments, on comprend pourquoi bon nombre de ces organisations se sont tournées vers l'automatisation des réseaux pour rester dans la course. Nous présentons ici une série de suggestions sur les aspects techniques de ces initiatives, ainsi que sur les raisons commerciales plus larges qui peuvent vous aider à convaincre les autres de la valeur des outils d'automatisation du réseau.

Pourquoi l'automatisation des réseaux est devenue incontournable

Pour illustrer les difficultés auxquelles vous êtes confronté en tant que responsable de l'administration de votre réseau, le mieux est sans doute d'évoquer des scénarios spécifiques dont nous ont fait part d'autres ingénieurs réseau.

Scénario X

Vous êtes responsable d'une petite équipe d'administration réseau pour une entreprise qui n'a que quelques années d'existence mais qui se développe rapidement. L'équipe est compétente, mais sa vedette est Dave, un as du code qui crée des scripts en Python pour gérer la configuration des nouveaux équipements et des nouvelles plates-formes. Jusqu'à présent, tout se passe bien. Puis un jour, Dave dit qu'il doit vous parler.

Dave se confie : « On m'a proposé un poste dans une autre entreprise, et ils doublent mon salaire. Donc je vais tout boucler dans les prochaines semaines. Désolé, mais je ne pouvais pas refuser. »

Vous avez l'estomac noué. Dans deux semaines, Dave sera parti, et personne d'autre dans votre équipe n'a autant de talent. Bien sûr, ils savent coder, mais pas comme Dave. Et étant donné la pénurie d'ingénieurs réseau talentueux, vous savez que vous n'êtes pas près de trouver un autre Dave.

Vous envisagez donc l'acquisition d'un outil d'automatisation du réseau – quelque chose qui fera le travail que Dave faisait sans être tenté par un salaire plus élevé, tout en améliorant les capacités de votre équipe réseau.

Ce n'est qu'un des nombreux scénarios qui mettent en évidence le rôle de plus en plus important que joue l'automatisation du réseau dans les entreprises modernes, quelle que soit leur taille. Quand votre réseau tombe en panne, vous n'avez aucun recours. Vous ne pouvez pas vendre de produits. Vous ne pouvez pas servir vos clients. Vous ne pouvez pas vraiment faire grand-chose en tant qu'entreprise.

Les coûts peuvent être faramineux. [L'Enquête 2021 sur le coût horaire des temps](#) d'arrêt de l'ITIC révèle que pour 91 % des entreprises, une seule heure d'arrêt coûte au moins 300 000 \$ en raison de la perte d'activité et de productivité, et du coût des mesures de correction. Pour 44 % des entreprises interrogées, ce chiffre se situe entre 1 et 5 millions \$ par heure.

D'autres enquêtes ont montré que ces pannes sont causées par des erreurs de configuration du réseau, elles-mêmes le plus souvent dues à des défauts dans des tâches manuelles.

Examinons d'autres scénarios qui pourraient vous amener à adopter une solution d'automatisation du réseau:

Scénario Y

Avant le départ de Dave, vous détectez une vulnérabilité affectant votre infrastructure réseau. Dave analyse rapidement la situation et voit où votre réseau pourrait être attaqué. Il découvre un logiciel malveillant qui vient d'infiltrer l'un de vos périphériques réseau ; il déconnecte rapidement

la machine touchée du reste du réseau et empêche le logiciel malveillant de faire des dégâts plus importants. Il télécharge ensuite un correctif auprès du fabricant de l'équipement et l'applique à tous les équipements du même type, sur l'ensemble du réseau. Mais vous réalisez que si Dave n'avait pas été là, personne d'autre n'aurait été capable de résoudre le problème.

Scénario Z

Le réseau tombe en panne à 16 heures et Dave a déjà pris ses nouvelles fonctions. Rien ne fonctionne – pas d'email, pas de Zoom, pas de Slack – si bien que tout le monde rentre chez lui. Le PDG est très clair : « Vous feriez mieux de nous remettre en ligne avant demain matin. » Aidé des membres junior de votre équipe vous travaillez frénétiquement toute la nuit pour restaurer le réseau manuellement, car les sauvegardes automatiques normalement collectées par les scripts Python de Dave ont cessé de fonctionner il y a quelques semaines, et il est le seul à posséder des compétences approfondies en développement logiciel.

Aborder l'automatisation des réseaux de manière stratégique

Soyons honnêtes, vous ne pouvez pas passer d'un processus d'administration de réseau largement manuel à une stratégie entièrement automatisée et totalement intégrée du jour au lendemain. Vous devez établir des priorités. Celles-ci seront différentes pour chaque entreprise, mais elles se répartissent en trois étapes de réalisation.

Première étape : Votre équipe et vous faites ce qu'il faut pour maintenir le bon fonctionnement du réseau et assurer une sécurité de base. Vous allez ainsi automatiser les sauvegardes de configuration, les procédures de restauration et de la validation des politiques.

Deuxième étape : Votre équipe et vous prenez des mesures pour être toujours plus efficaces et réduire les coûts. Cette fois, vous allez automatiser l'optimisation de l'état de santé, des performances et de la sécurité de votre infrastructure réseau.

Troisième étape : À ce stade ultime, votre équipe et vous pouvez vous concentrer sur la gestion de la plate-forme d'automatisation et sur l'approbation des changements. L'automatisation, elle, va prendre en charge la majeure partie du travail que vous assumiez auparavant. Vous allez donc automatiser les transferts, ajouts et modifications demandés par les utilisateurs, car la plate-forme elle-même répond directement aux tickets ServiceNow et aux demandes des utilisateurs.

Vous souhaitez certainement avancer aussi vite que possible, mais il est essentiel de se concentrer d'abord sur les tâches pratiques et essentielles. Si une panne paralyse votre entreprise pendant plusieurs jours ou si elle subit une violation majeure qui entraîne la fuite de données personnelles de vos clients, vous pouvez oublier les réductions de coûts et les gains

Détendez-vous, vous n'êtes pas le seul à dépendre de processus manuels pour vos activités [réseau](#). Selon Gartner, en 2022, moins de 35 % des activités réseau sont automatisées.

Voyons donc quelles activités de réseau doivent être abordées, en commençant par la première étape avant de passer à la deuxième. La troisième étape est si éloignée pour la plupart des équipes qu'il n'est pas nécessaire d'en parler à ce stade.



Fonctions de sauvegarde et de restauration

Quelle que soit la nature de votre réseau, vous devez être en mesure d'exécuter les fonctions de sauvegarde et de restauration nécessaires au bon déroulement de vos opérations. Il s'agit incontestablement d'un problème à aborder dès la première étape. Si vous n'automatisez pas les fonctions de sauvegarde et de restauration, vous exposez votre entreprise à un risque important de temps d'arrêt.

Les systèmes d'automatisation du réseau éliminent les difficultés liées aux processus manuels de sauvegarde et de restauration. Sa fonction de réduction des coûts pourrait classer cette démarche dans l'étape 2, mais il est à noter que toute perturbation du fonctionnement d'une entreprise impacte encore plus ses finances et sa réputation. Considérez-la donc comme une exigence de l'étape 1.



Contrôle des changements de configuration

Les plates-formes d'automatisation des réseaux doivent être capables de détecter quand des changements sont nécessaires ou quand l'ingénieur réseau doit être informé des changements. Quel que soit l'outil de configuration que vous achetez à cette fin, il doit être intégré à l'écosystème global de gestion informatique. Le critère de base est la capacité de configuration et les tâches qui y sont associées : la validation et les tests.

Un outil de configuration automatisé améliore considérablement la contribution de vos ingénieurs réseau débutants. L'outil comprend des rails de sécurité intégrés qui empêchent l'ingénieur inexpérimenté de commettre des erreurs préjudiciables. Il peut ainsi accomplir beaucoup plus chaque jour qu'il ne l'aurait fait en s'appuyant sur des processus manuels. Parce qu'elle peut éviter à un employé débutant de commettre une erreur grave et lourde de conséquences, cette exigence relève de la première étape.



Gestion de l'inventaire

Le service d'administration du réseau doit s'assurer que tous les appareils du réseau sont correctement inventoriés afin que l'ingénieur puisse tous les voir en même temps, s'y connecter si nécessaire et agir au besoin. Ici, la tâche essentielle du service est d'établir un inventaire exhaustif, ainsi qu'un processus qui assure la régularité et la mise à jour de l'inventaire.

Ce processus variera d'une entreprise à l'autre, mais il doit inclure comme point de départ un moyen d'établir des communications dans toute l'entreprise afin que les ingénieurs réseau soient informés en cas d'ajout, de problème opérationnel, etc. Il doit également comporter un ensemble défini de principes servant à collecter les informations clés. Par exemple, les conventions de dénomination des dispositifs, des bases de données, des services, etc., doivent être unifiées afin de minimiser la confusion et les travaux futurs inutiles.

Il s'agit d'une fonction quelque peu avancée, qu'on pourra plutôt traiter en dernière partie de la première étape.



Automatisation de la sécurité

En raison de la menace croissante que représente la cybercriminalité, il est important que l'ingénieur réseau confirme continuellement le périmètre de sécurité de l'entreprise en s'assurant que les pare-feu et les systèmes de détection des intrusions remplissent leur fonction. En outre, le système d'automatisation de la sécurité doit s'intégrer à un flux de menaces, à une protection des terminaux et à des plateformes de détection et réponse étendues (XDR). Il s'agit là aussi de la première étape, mais la sécurité étant une proposition sans fin, c'est une tâche qui n'est jamais terminée.



Automatisation du centre de données

Les centres de données modernes mélangent infrastructures physiques et virtuelles et évoluent rapidement pour fonctionner de plus en plus comme un cloud public. L'automatisation des transferts, ajouts et modifications (MAC en anglais) exige de pouvoir couvrir plusieurs dispositifs et repose lourdement sur l'automatisation de l'infrastructure informatique. Le nombre de MAC requis dans les centres de données modernes nécessite une stratégie d'automatisation complète. Pourtant, le risque posé par un changement seul est moindre que celui des changements au niveau de l'infrastructure, qui relèvent de l'étape 1.

La plupart des entreprises tireront profit d'une automatisation robuste du cloud, généralement dirigée par les équipes des opérations cloud, DevOps ou d'ingénierie de la fiabilité des sites. Ces outils centrés sur les systèmes d'automatisation orientés calcul peuvent s'intégrer aux meilleurs outils d'automatisation de l'infrastructure réseau, afin d'automatiser l'ensemble des changements requis.

Un autre facteur à prendre en compte : à terme, le centre de données et les données cloud seront probablement gérés à l'aide d'une superposition de services maillés. La tendance est à l'adoption d'une méthode unique de contrôle des environnements physiques et virtuels, et le concept de maillage de services est sans doute la méthodologie qui sera employée à cette fin.

Facteurs supplémentaires qui motivent la planification de l'automatisation du réseau

Facteurs liés à la conformité

La conformité aux réglementations en vigueur est une préoccupation extérieure majeure pour tous les services informatiques et de sécurité. Par exemple, pour des raisons de confidentialité et de sécurité, l'ingénieur peut souhaiter disposer de capacités de gestion des accès privilégiés.

Les sociétés de services financiers, les entreprises des télécommunications et des médias, les fournisseurs de services gérés et les fournisseurs de services de sécurité gérés sont autant d'exemples d'organisations qui doivent être attentives aux questions réglementaires. La liste des secteurs soumis à des réglementations ne fera que s'allonger au fil du temps.

N'oubliez pas les conséquences juridiques potentielles du non-respect des exigences de conformité.

Une violation de la vie privée peut entraîner un procès coûteux, car la non-conformité devient une preuve solide contre votre entreprise.

En plus de la conformité externe, il y a des questions de conformité interne à prendre en compte. Par exemple, vous voulez vous assurer que tous les serveurs NTP dans la configuration des équipements sont définis sur 10.0.0.1.

Facteurs liés à la vitesse de déploiement

Relatively few organizations can afford long delays in
Peu d'organisations peuvent se permettre de longs retards dans leur implémentation de l'automatisation de réseau. Les retards ne font que compliquer les problèmes et empêchent l'équipe de répondre efficacement aux situations pour lesquelles les outils d'automatisation de réseau sont conçus.

Il faut donc sacrifier certaines fonctionnalités de personnalisation au profit d'un déploiement rapide.

C'est un choix que beaucoup d'entreprises de taille moyenne sont plus qu'heureuses de faire, car elles sont déjà surchargées et ne peuvent pas se permettre de nouveaux retards. Le rapport temps-valeur est un facteur déterminant dans ce cas.

Facteurs liés au débit du réseau

Pour certaines entreprises, les temps de réponse quasi instantanés des applications en contact avec la clientèle sont essentiels. Si vous vendez un article en ligne dans un domaine concurrentiel, un retard d'exécution peut inciter les acheteurs à abandonner leur panier et à se connecter sur le site d'un rival. Dans ce cas, vous pouvez envisager des outils qui permettent de surveiller les performances et les défaillances de votre réseau.

La souplesse d'une API ouverte

Plutôt que de dépendre d'un seul fournisseur, un système d'API ouverte permet aux administrateurs de réseau de choisir des fournisseurs différents pour chacune des fonctions de leur système. Cela permet également aux organisations d'ajouter des fonctionnalités au fil de leurs besoins.

Il est tout simplement irréaliste de penser qu'un seul fournisseur ou système propriétaire peut répondre à vos besoins en matière d'infrastructure informatique. Certains de vos collaborateurs auront leurs outils préférés.

Vous devez veiller à la compatibilité de tout ce que vous achetez pour l'administration du réseau.

Facteurs liés aux coûts

Face aux pressions exercées pour faire plus avec moins, les équipes informatiques doivent trouver des solutions qui les aident à accomplir leur travail sans épuiser leur budget. Une solution qui répond aux attentes et qui permet à l'organisation de se développer et d'ajouter des outils si nécessaire est un moyen efficace de résoudre ce problème.



À propos de BackBox

Backbox a pour mission de permettre à ses clients d'améliorer en permanence la robustesse, les performances et la sécurité de leur infrastructure réseau grâce à une automatisation intelligente et axée sur la sécurité. Nous pensons que l'automatisation des réseaux doit être facile et accessible, et offrir à nos clients un gain de temps considérable tout en réduisant les risques.

Pour en savoir plus, consultez BackBox.com.